Nortel Threat Protection System SEU/Rule Update

Date: 2007-07-17

This update is SEU 87 for the 4.5 and 4.6 series of the Defense Center and Intrusion Sensor.

This update applies to all 4.5 and 4.6 models of the Defense Center and Intrusion Sensor.

This SEU contains an updated detection engine that includes new features and functionality.

These release notes describe:

- New Features and Functionality
- Known Issue

New Features and Functionality

SEU 87 contains an updated detection engine and includes the following new features and functionality:

- Stream 5 Preprocessor
- SEU Rollback and Forced Install

Stream 5 Preprocessor

The Stream 5 preprocessor provides next-generation TCP stateful inspection and stream reassembly for Intrusion Sensors and Defense Centers using Version 4.6.0.2 or greater. Thirteen distinct operating system profiles allow you to tailor Stream 5 to reassemble traffic for inspection precisely the way it is reassembled by the different operating systems used by the hosts on your monitored network. This provides your Intrusion Sensor's detection engine with more accurate TCP data for analysis. Stream 5 can also identify and track UDP sessions by using the source and destination IP addresses in the encapsulating IP datagram header and the port fields in the UDP header. Stream 5 also provides improved memory management, multiple buffer flushing data models, and improved TCP timestamp support. Stream 5 will eventually replace the Stream 4 preprocessor, which was known as the Stateful Inspection and Stream Reassembly preprocessor until the introduction of Stream 5. Stream 5 also incorporates all of the functionally of the flow preprocessor, required by Stream 4, and will replace it as well.

SEU Rollback and Forced Install

This SEU provides two features that can assist you with certain requests for Support assistance. SEU Rollback allows you to remove the most recently installed SEU and install the SEU that preceded it. The Forced Install feature allows you to reinstall the currently installed SEU, which can be useful, for example, when an import fails because it is interrupted for some reason. Contact Support for assistance if you encounter problems importing an SEU.

Known Issue

The following is a known issue with SEU 87:

- Although the SEU installs the Stream 5 configuration options for Versions prior to Version 4.6.0.2, Nortel strongly recommends that you use the Stream 5 preprocessor **only** for Version **4.6.0.2 or greater**. Enabling Stream 5 on versions prior to 4.6.0.2 may impact the sensor's performance.

WARNING: Nortel Threat Protection System customers must upgrade to 4.5.1 prior to applying this patch. Failure to upgrade will result in sensor failure when installing these rules.

Snort Engine Updates: In Threat Protection System v4.1, Snort Engine Updates (SEUs) replaced rule pack updates as the mechanism for updating Snort and Snort-based rules. In addition, SEUs can provide new and updated preprocessors and protocol decoders that aid in detecting intrusion attempts.

Note that SEUs can contain new binaries (in the form of shared object rules and new versions of Snort), so make sure that your process for installing new SEUs complies with your network and security policies.

Shared Object Rules: Shared object rules (SORs) are a new type of rule that allows the Nortel Threat Protection System Team more flexibility in detecting possible intrusions. SORs are delivered in SEUs in binary format as compared with the text rules (now called standard text rules or STRs) that were provided in previous rule packs.

You can view the rule documentation and create copies of shared object rules just as you could with standard text rules. However, you can only view and modify attributes such as the message or the source and destination ports and addresses in the rule header. You cannot view or modify the rule keywords section, including rule content keywords. Note that you can still create and modify your own standard text rules, and you can view, copy, and modify any of the legacy standard text rules.

How to get help: If you have purchased a Nortel service program, contact Nortel Technical Support. To obtain contact information online, go to www.nortel.com, and then click on Technical Support.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, you can call 1-800-4 NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to http://www.nortel.com/support . Click on the link for Express Routing Codes located at the bottom-right corner of the Web page.